



SATERN

System for Administration, Training, and Educational Resources for NASA

Managing Access

Classroom Guide

(Version 5.8 SP5)

April 2010





For SATERN v 5.8 SP5

Last Modified 04/28/2010

The software described in this document is furnished under a license agreement. The software may be used only for learning and development purposes of the NASA employees. No part of this training may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express written permission of NASA.

From the NASA SATERN Program Office:

All SATERN administrator training materials must be used alongside the SATERN Rules and Process Guide for administrators. The Guide identifies areas where SATERN functionality cannot enforce the Agency-defined usage of the system at NASA and provide guidance to enable administrator compliance with Agency-defined methods and procedures.



Table of Contents

Course Introduction	1
Course Objectives	1
Target Audience	1
Using this Guide	1
Additional Resources.....	2
Lesson 1: Administrator Access.....	3
Objectives.....	3
Administrator Access Overview	3
Terms and Definitions	5
Workflows	5
Admin Roles	6
Administrator	7
Domains	8
Domain Restriction	9
NASA Domain Structure	11
NASA Sample Domain Restriction.....	12
Conclusion.....	12
Lesson Check.....	13
Lesson 2: Managing Roles	15
Objectives.....	15
Overview of Workflows and Roles	15
Workflow	15
Roles	16
Granting Administrative Rights	21
Conclusion.....	21
Lesson Check.....	22
Lesson 3: Managing Administrators	23
Objectives.....	23
Overview of Admin Management.....	23



Admin Records	24
Preferences Tab	24
<i>Lab 1. Creating an Admin Account – Refer to business rule</i>	<i>25</i>
Conclusion.....	27
Lesson Check.....	28
Lesson 4: Learner Access	29
Objectives.....	29
Learner Access to Menus	29
SATERN Learner Roles.....	29
Learner Access to Items and Scheduled Offerings.....	30
Catalogs.....	30
<i>Lab 2. Add a New Catalog</i>	<i>31</i>
Granting Learners Access To a Catalog.....	32
Conclusion.....	33
Lesson Check.....	34
Course Summary.....	35



Course Introduction

Through lecture, activities, and hands-on computer lab work, this course teaches you the concepts and terminology associated with security management in SATERN. You gain hands-on experience using the system functions in order to create and modify the security structure.

COURSE OBJECTIVES

Upon completion of this course, you will be able to:

- Describe the security model in SATERN
- Understand the purpose of domains and domain restrictions
- Describe learner roles and access to catalogs

TARGET AUDIENCE

This training is intended for SATERN administrators responsible for setting up and maintaining security in the SATERN system.





USING THIS GUIDE

This classroom guide is designed to be used in conjunction with an instructor. The guide provides general information that will be elaborated upon by the instructor. For additional information, refer to the online help.

Throughout the guide, you encounter icons that call out various types of information. The following table illustrates how this guide



uses icons to indicate different types of comments, activities, labs, etc. that support the text.

Icon	Definition
	Activity: Indicates an activity for you to complete that helps reinforce the information you just learned.
	Note or Tip: Indicates additional information that is related to the information presented. It also provides helpful hints and tips or other guidance that further explains the information it accompanies.
	Lab: Indicates a hands-on computer lab. Follow the step-by-step process outlined to perform specific tasks in the system.
	Warning: Warns against particular actions, or that a particular condition might indicate a problem.

ADDITIONAL RESOURCES

There are a number of additional resources that can provide you more information about the SATERN system. These resources include:

- ◆ Online SATERN system help
- ◆ Task-specific job aids



Lesson 1:

Administrator Access

The goal of this lesson is to establish a general understanding of the concepts and terminology associated with administrator (admin) access in the SATERN system.

OBJECTIVES

Upon completion of this lesson, you will be able to:

- Define a domain
- Define a domain restriction
- Define a workflow
- Define an admin role
- Define an admin
- Illustrate the relationships between domains, domain restrictions, workflows, roles, and administrators

ADMINISTRATOR ACCESS OVERVIEW

SATERN employs a multi-level security model. This model allows administrators to perform various functions in the SATERN system by restricting the functions to specific groups of data. Each of these topics is discussed in detail later in this course.



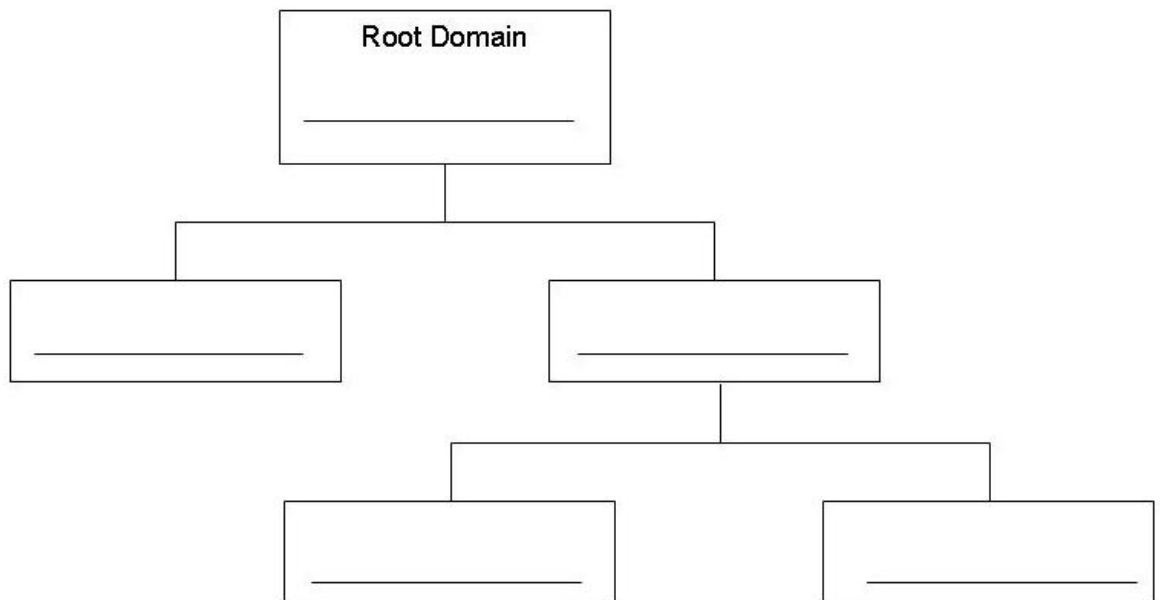
Activity

To help you understand how admin access works, the instructor will begin an interactive discussion. You will be asked to describe an administrative role in their organization. Once an admin role is agreed upon, you will list several things a person with that admin role may be asked to do in the SATERN system. You will also consider the admin organization's domain structure and how domain restrictions are used.

Populate this chart with the information discussed in class:

Admin Role: _____

	Function	Entity
Workflow:		
Workflow:		
Workflow:		
Workflow:		
Workflow:		



Keep this chart handy for the rest of this course.



Terms and Definitions

Table 1 lists the terms and definitions associated with administrator access in SATERN.

Table 1. Administrator Access Terms and Definitions

Term	Definition
Administrators	An individual that has an assigned role and responsibility in SATERN to manage system data. (<i>who</i>).
Domains	A data 'location' that determines admin ownership. Domains are used to control all records, including learner records in the database (<i>what an administrator can see or where he/she has access</i>).
Domain Restrictions	A record that determines in which domains an administrator may perform assigned workflows.
Domain Types	The types of entities that are controlled by domains.
Roles	A group of workflows.
Workflows	Functions an administrator can perform on entities within SATERN (<i>what an administrator can do</i>).

WORKFLOWS

Workflows are functions an admin or learner can perform within the SATERN system. Workflows can range from viewing objective data to recording learning events for learners.

A workflow is comprised of a function tied to an entity. Functions are actions, such as “add,” “view,” “edit,” “copy,” “search,” and “delete.” Examples of entities in the system include “items,” “learners,” and “scheduled offerings.” The combination of a function applied to an entity is a workflow.

For example, a workflow might be “view items.” Other workflows include “edit learners” and “delete scheduled offerings.” There are between 750 and 900 workflows that exist to match what administrators and learners may do in the system. The exact number depends on which modules of SATERN you may be using.



Each workflow in an admin role can be assigned a domain restriction, limiting access to only the domains listed in the domain restriction (Figure 1).

Workflow		
Function	Entity	State
View	Learner	Active/Inactive/Both
Add	Learner	Active/Inactive/Both
Edit	Learner	Active/Inactive/Both
Delete	Learner	Active/Inactive/Both

Figure 1. Workflows

ADMIN ROLES

An admin role is simply a collection of workflows. One or more workflows can be set up as an admin role, and the role can then be assigned to an admin.

By breaking down SATERN system access to the combination of the workflows and domains assigned to an admin, extreme granularity is built within the existing security model, allowing you to control access to features and data as precisely as desired (Figure 2).

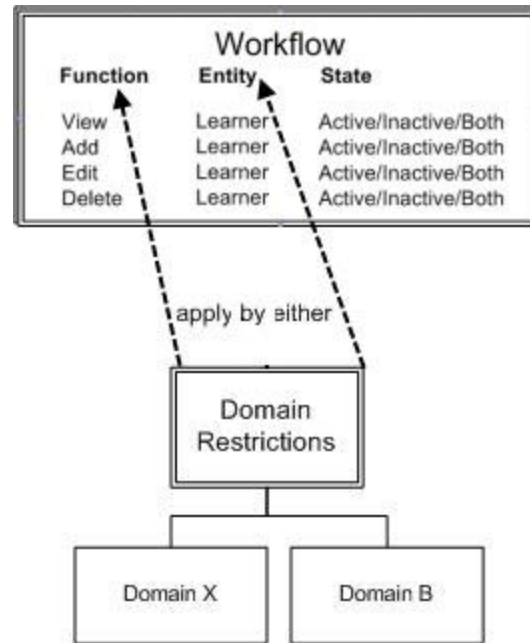


Figure 2. Roles

ADMINISTRATOR

The administrator is assigned one or more admin roles, allowing the re-usability of roles (Figure 3). Each admin has preferences, including an active locale ID and time zone ID. The locale determines standards such as number patterns; the time zone determines how times are displayed to the admin. The admin may check the **Always display Schedule Offerings in this Time Zone** checkbox in order to override the specific time zone settings for each scheduled offering.

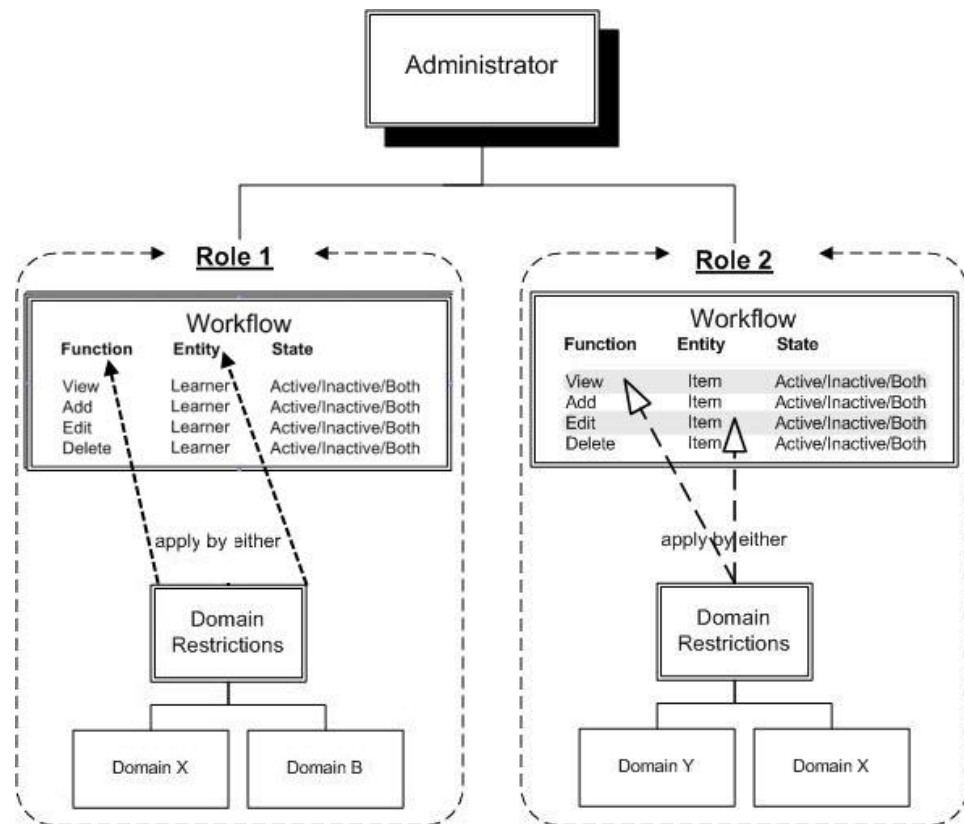


Figure 3. Admin with Two Roles

DOMAINS

The use of domains is an important part of the security strategy. Domains are used to indicate where the data resides and helps you determine who can access what data. Domains allow for compartmentalization of data records in the database and define what an admin can see or where in the system he/she has access. Domains act as active filters for data, allowing only admins with roles that include access to specific domains to view or manipulate the data associated with those domains.

Most entities in SATERN (also called *domain types*) can be associated with domains. When an entity is created, exactly one domain may be specified.

Domains can be built in a linear, hierarchical structure, with each domain having one or more children. Each domain can have only one parent. The nested structure allows administrators to access data within organizational structures with minimal work (Figure 4).

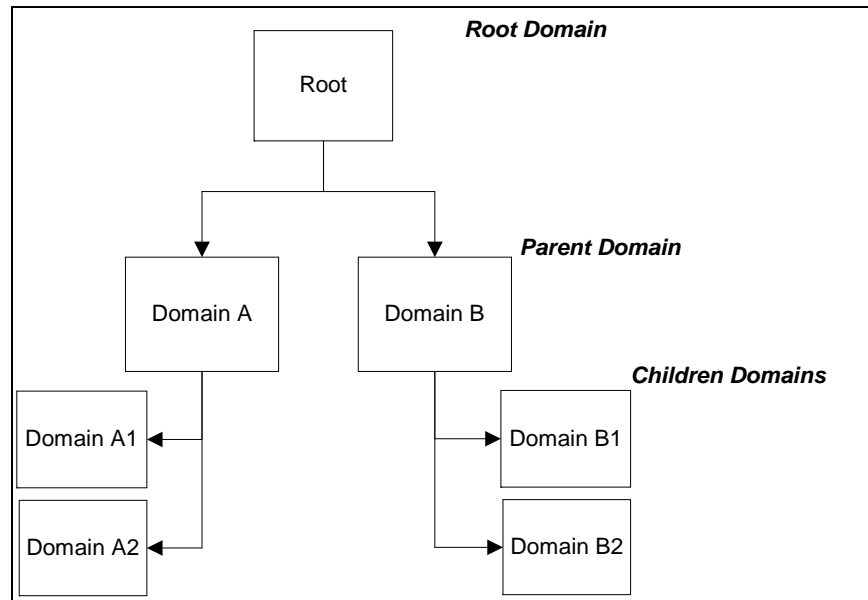


Figure 4. Domains

DOMAIN RESTRICTION

Individual domains can be included in a domain restriction, which is a group of domains. A domain restriction allows access to a particular set of data; for example, access to just the specified domain or the specified domain and all of its child or sub-domains.

The development strategy for domains can be approached in two ways:

- ◆ “Broad Domain” strategy: May reduce the administrative burden by keeping the number of domains and domain restrictions to a minimum

- ♦ “Narrow Domain” strategy: Increases the specificity of domain security, but increases the number of domains and domain restrictions that must be created and assigned

A domain restriction is used in conjunction with workflows to specify what an admin can do to the data he/she can access (Figure 5).

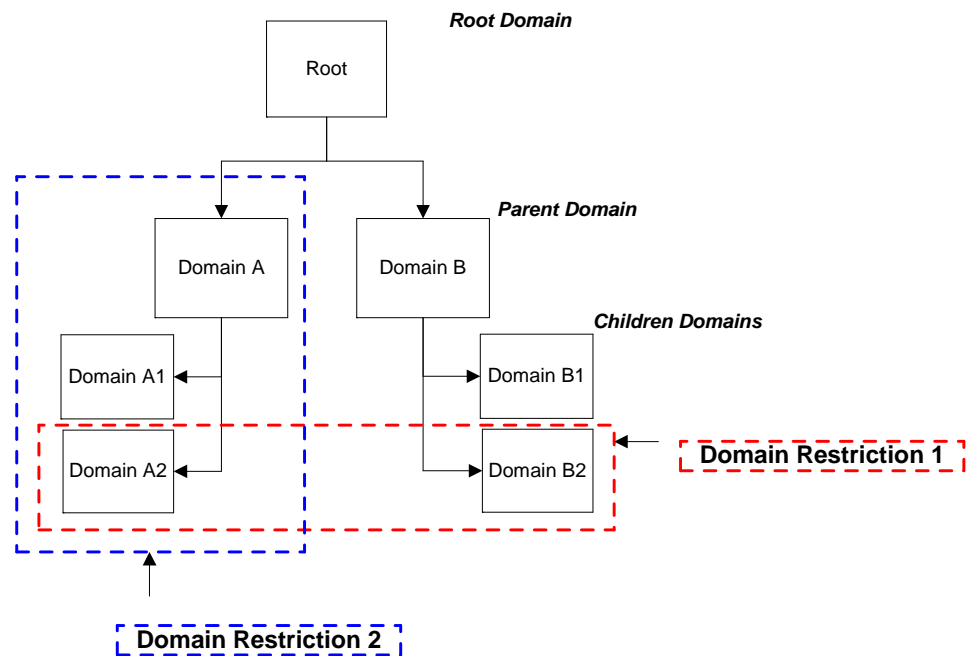


Figure 5. Domain Restrictions

NASA Domain Structure

Figure 6 depicts the NASA domain structure.

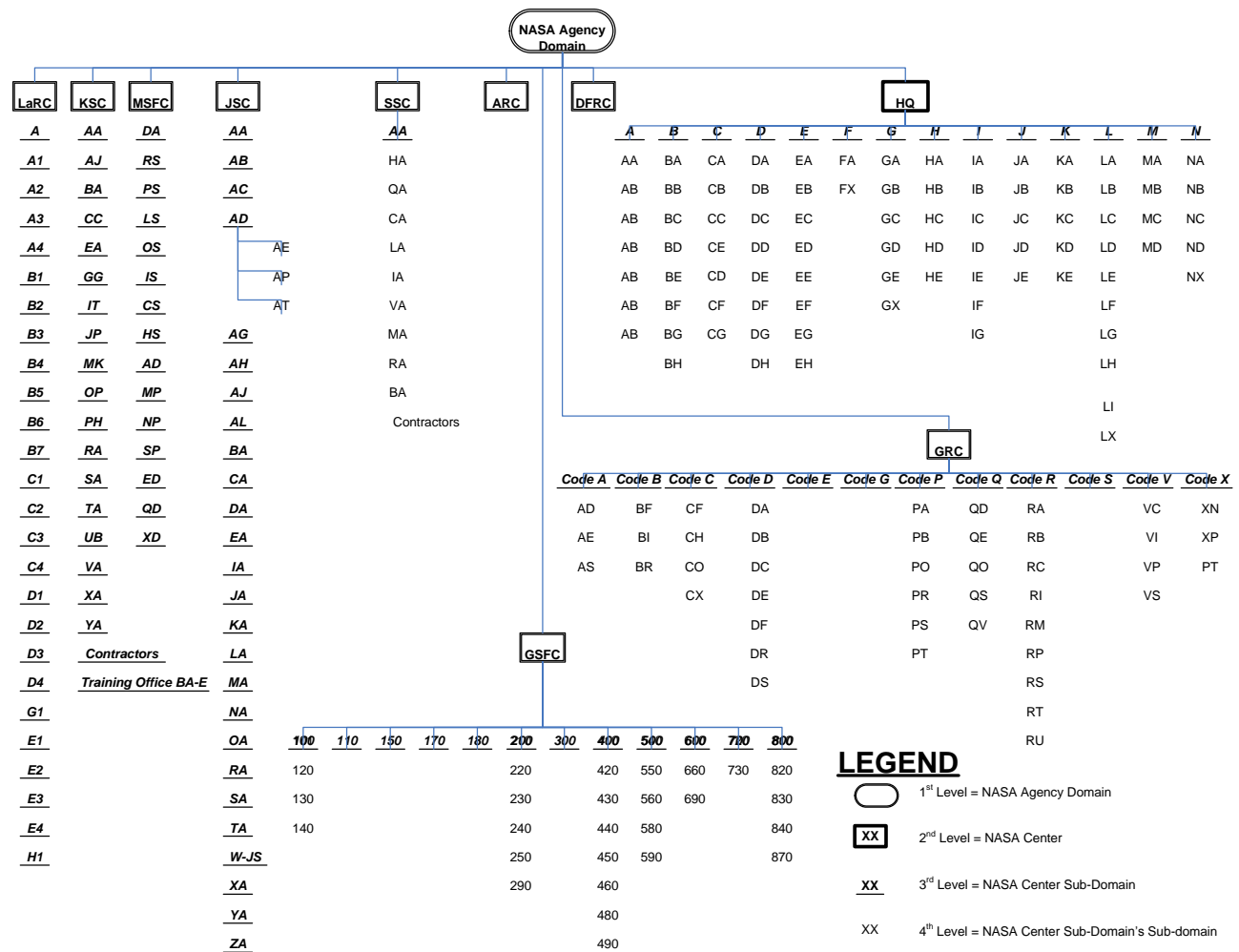


Figure 6. NASA Domain Structure

NASA Sample Domain Restriction

Figure 7 shows a sample of a NASA domain restriction.

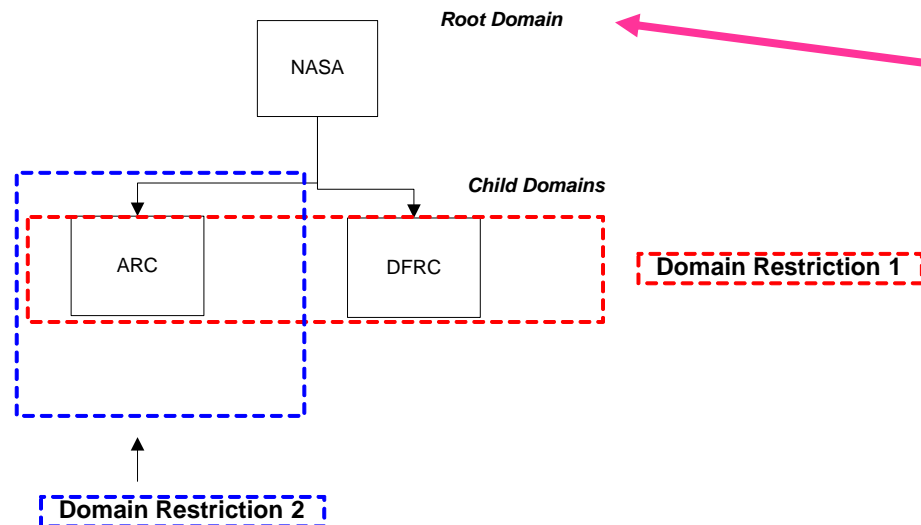


Figure 7. NASA Sample Domain Restriction

CONCLUSION

In this lesson, you were introduced to the general concepts and terminology associated with admin access in the SATERN system.

You should now be able to:

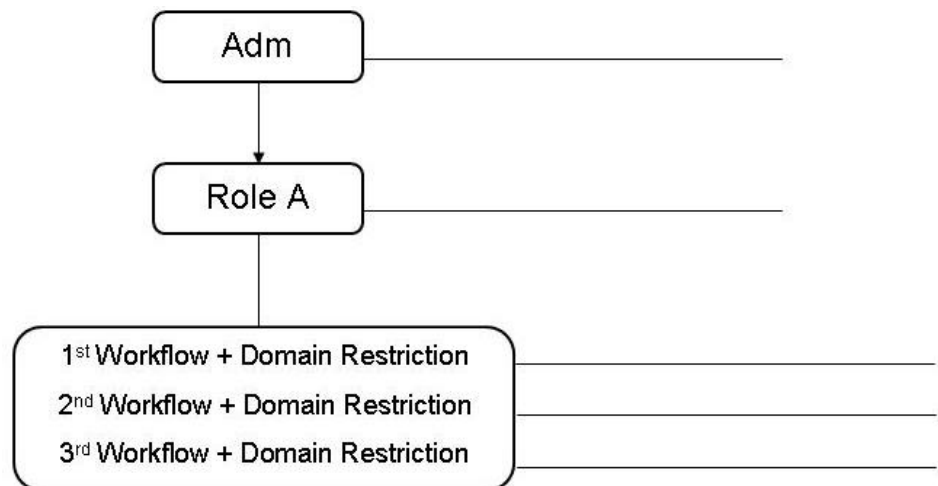
- Define a domain
- Define a domain restriction
- Define a workflow
- Define an admin role
- Define an admin
- Illustrate the relationships between domains, domain restrictions, workflows, roles, and administrators

In the next lesson, you will explore roles and how to work with them.

LESSON CHECK

Use what you learned in this lesson to answer the following questions.

1. In the diagram below, fill in an example for an admin, the role you would assign to him/her, and three workflows with associated domain restrictions that would be added to this role. Keep in mind that you could potentially assign over 750 workflows! Just keep it simple for this activity.



2. A SATERN system workflow is:
 - a) A responsibility of a member of the company security department.
 - b) A responsibility related to company security similar to locking procedures.
 - c) A function given to all learners.
 - d) Permission for a specific action in SATERN administration.



3. In the SATERN system, a domain:
 - a) Allows admins to perform certain functions.
 - b) Identifies a data set.
 - c) Identifies security functions.
 - d) Allows an admin access to certain records.

4. In the SATERN system, a domain restriction:
 - a) Includes all domains created.
 - b) Includes the domains you don't want your administrators to view.
 - c) Is customized to include whatever domains the admin needs to have access to.
 - d) Can only include children domains.

5. A role can be defined as:
 - a) A collection of workflows.
 - b) A job description.
 - c) The data that one can see.
 - d) A restriction.



Lesson 2:

Managing Roles

The goal for this lesson is to provide detailed information about roles and how to create and work with them in the SATERN system.

OBJECTIVES

Upon completion of this lesson, you will be able to:

- Identify the purpose of a workflow
- Describe the importance of roles
- Describe how roles relate to workflows

OVERVIEW OF WORKFLOWS AND ROLES

As discussed in the previous lesson, workflows are functions an admin or learner can perform on entities within the SATERN system. Roles are groups of workflows.

Workflow

A workflow is a specific set of data manipulation permissions that allow the admin or learner to perform specific actions. When creating a role administrators may choose from over 750 predefined workflows.

Roles

A role is a group of workflows defined by a role. A role gives administrators the ability to create virtually an unlimited number of distinct functions.

NASA Roles

This section provides a high-level overview of the generic roles which are available. Each role may be used differently at each center. The capabilities of each role include:

- ◆ Super Administrator
 - Most robust administrator role in the system. The Super Administrator has full access to all workflows in all domains.
- ◆ Level 1: Regional Administrator
 - The Level 1 Training Lead has access to every workflow within SATERN, with the exception of those that affect global settings or global reference tables.
 - A Level 1 Training Lead is assigned to each Center Domain (the generic Training Lead Role is copied for the domain-specific role, and modified as needed).
 - Rights of the Level 1 Training Lead include:
 - Manage items, content objects, and curricula
 - Manage scheduling and resources
 - Manage learners
 - Manage catalogs and commerce functions
 - Manage most system administration functions
 - Run reports



NASA Business Rule

There is a limit of three (3) Level 1 administrators for each center and discipline. The Level 1 administrator is the only role that may create administrator accounts for other administrators.

Level 1 administrators may create lower-level administrator accounts for administrators at their centers or within the discipline but must notify the Center Training Office or the Center PoC of the account that was created. If other Level 1 accounts are desired at a center or within a discipline, the center or discipline SAL must forward the recommendation to the SATERN Agency Operational Support Lead listed on the SATERN Informational Web site (https://saterninfo.nasa.gov/Organization_Project_Team.html). Once approved, the SATERN Operational Support Lead forwards the request to the NSSC for creation of the new RA-1 account.

◆ Level 2: IT Administrator

- The Level 2 role is for troubleshooting.
- Rights of the Level 2 role include:
 - Most system administration capabilities
 - Most learner management capabilities
 - Change email address
 - Give learner his/her password and learner ID
 - Add and edit learner profile/new accounts and ability to edit/copy learners and custom columns
 - Able to view/edit custom columns
 - View and search everything

◆ Level 3: Training Office Administrators

- The Level 3 role is primarily responsible for managing and tracking learner training needs, though they also have access to create items and scheduled offerings.



- Rights of the Level 3 role include:
 - Manage items, content objects, and curricula
 - Manage scheduling and resources
 - Manage learners, schedule courses, edit assessment instances, reserve equipment
 - Manage catalogs
 - Run reports
- ◆ Level 4: Organization Training Coordinator
 - The Level 4 role is primarily responsible for creating courseware, items, and if needed, scheduled offerings.
 - Rights of the Level 4 role include:
 - Manage items, content objects, and curricula
 - Manage scheduling and resources
 - Run reports
- ◆ Level 5: Manage Facilities
 - The Level 5 role is primarily responsible for managing resources.
 - Rights of the Level 5 role include:
 - Manage resources (instructors, facilities, etc.)
 - Run limited reports
- ◆ Level 6: Manage Commerce (not for Phase II)
 - The Level 6 role is primarily responsible for managing financial aspects of training, such as training costs.
 - Rights of the Level 6 role include:
 - Manage commerce
 - Run limited reports
- ◆ Level 7: First Tier Help Desk
 - The Level 7 role is primarily for end-learner troubleshooting.



- Rights of the Level 7 role include:
 - Limited system administration capabilities
 - Limited learner management capabilities
 - Reset passwords and notify learners of their learner ID.
 - Change email address
 - Search, view, and edit learner records
 - Search and view almost anything about a learner and custom columns
- ◆ Level 8: Discipline Domain Administrator
 - The Level 8 role is primarily for managing learner histories and running reports for their domain.
 - Rights of the Level 8 role include:
 - Search and view learners
 - Search and view items and completion status
 - Run item status reports
 - Ability to add, view, copy and delete items, catalogs, and curricula
 - Search and schedule scheduled offerings and learner registration
 - No access to custom columns (specific to learner custom columns)
 - View, edit, and assign items to learner
- ◆ Level 9: Discipline Domain Reporter (RGI-type user)
 - The Level 9 role is primarily for viewing learner histories and running reports for their domain.
 - Rights of the Level 9 role include:
 - Search but not view learners
 - Search and view items and completion status
 - Run item status reports



Given Privacy Act constraints and domain controls in SATERN, only the Help Desk can create Level 8 and Level 9 Discipline Administrators. Since the Help Desk can neither verify nor authorize discipline administrative accounts in SATERN, the Discipline SAL must be responsible for those tasks.

NASA Business Rule

Discipline SALs can authorize discipline administrator accounts in SATERN. Level 1 administrators at the Center can also authorize and assign only the View Discipline Items role to their lower-level administrators at the Center.

Process: Anyone requesting full discipline administrator access must make the request to the Discipline SAL. Once the Discipline SAL verifies and authorizes the account, he/she will send an email to the NSSC Contact Center (NASA-SATERN.support@nasa.gov) requesting that the account be created. For those individuals who request an administrator account directly from the Help Desk, he/she will be directed to the appropriate Discipline SAL for action. For those requesting the View Discipline Items role to search and view items, contact your Center SAL.

- ◆ Level 11: View Only (Reports)
 - The Level 11 role is primarily “view only,” although this role may also run most reports.
 - Rights of the Level 11 role include:
 - Run reports
 - System has been adjusted so that this level cannot view custom columns such as race, etc.



Note: An administrator may have different levels for different domains. For instance, an administrator can have a Level 7 for Marshall, Level 5 for Goddard, and Level 2 for the Information Technology Security Discipline Domain. These roles can be modified, deleted, or added to at any time. There is no limit to the number of administrators assigned to each role.



Granting Administrative Rights

NASA Business Rule

Any requests for modification to existing Center/Discipline administrator assigned roles and/or the creation of new SATERN administrator accounts must be routed to the Center or Discipline SAL.

Center SALs are responsible for setting up new SATERN administrator accounts in the Production, Staging, and Training environments. Discipline SALs are required to work with the NSSC in setting up new and modifying existing SATERN administrator accounts for all appropriate environments.

CONCLUSION

In this lesson, you were introduced to the role management functionality and the key things to consider when creating a new role. Using the step-by-step instructions, you created a new role.

You should now be able to:

- Identify the purpose of a workflow
- Describe the importance of roles
- Describe how roles relate to workflows

In the next lesson, you will learn how to create and manage administrators in the SATERN system.



LESSON CHECK

Use what you learned in this lesson to answer the following questions.

1. Workflows are:
 - a) What an admin can do within the SATERN system.
 - b) A specific set of data manipulation permissions that allow the admin to perform specific actions.
 - c) Comprised of a function tied to an entity.
 - d) All the above.

2. Workflows and roles are important because they:
 - a) Determine which domain(s) an admin can see.
 - b) Determine what an admin can do.
 - c) Determine what a learner can see.
 - d) Determine what a learner can do.
 - e) Both B and D.

Lesson 3:

Managing Administrators

The goal for this lesson is to provide detailed information about administrators, including how to create and manage them in the SATERN system.

OBJECTIVES

Upon completion of this lesson, you will be able to:

- Identify the effect of a role on an admin account
- Apply multiple roles to an admin account

OVERVIEW OF ADMIN MANAGEMENT

The admin management menu option of the *System Administrator* menu allows administrators to create admin accounts. The admin name entered during set-up will be used by the admin to log in to SATERN administrator.

NASA Business Rule

Level 1 administrators may create lower-level administrator accounts for administrators at their centers or within the discipline, but must notify the Center Training Office or the Center PoC of the account that was created. If other Level 1 accounts are desired at a center or within a discipline, the Center or Discipline SAL must forward the recommendation to the SATERN Agency Operational Support Lead listed on the SATERN Informational Web site (https://saterninfo.nasa.gov/Organization_Project_Team.html).



Once approved, the SATERN Operational Support Lead will forward the request to the NSSC for creation of the new RA-1 account.

ADMIN RECORDS

An administrator record contains:

- ◆ One or more roles assigned to the administrator account
- ◆ Record information that will enable the administrator to send and to receive system notifications

NASA Business Rule

Administrator IDs should follow the learner ID format (lower case, first initial, middle (second) initial, last name).

The administrator will only be able to perform those functions for which he/she has been specifically granted permission. If the role assigned to the administrator does not include certain permissions, such as view, the administrator is not able to use SATERN, because he/she does not have permission to view data.

Preferences Tab

Set the active locale and time zone to indicate the time zone in which operations occur and which language, time, and date settings the administrator sees. The **Always Display Scheduled Offerings in this Time Zone** checkbox should only be checked if the administrator wants to override the time zone settings of each individual scheduled offering. The settings can be set so that either all learners and administrators see a specific time zone, or each learner and administrator sees his/her particular time zone.



Lab 1. Creating an Admin Account – Refer to business rule

Add an Administrator Admin Account

Step

1. Navigate to **System Admin > Application Admin > Admin Management**.
2. Click **Add New**.
3. Enter an admin ID.
4. Enter new administrator's last name, first name, and middle initial.
5. Enter administrator's UUPIC number.
6. Enter administrator's email address.
7. Click the **Add** button.

Assign Role(s) to the Admin Account

Step

1. Select the **Assigned Roles** tab.
2. Click the **add one or more from list** link.
3. Enter search criteria to search for the desired role(s) for the admin.
4. Click **Search**.
5. Check the **Add** checkbox next to each role to add to this admin account.
6. Click the **Add** button.



Set the Admin Preferences

Step

1. Select the **Preferences** tab.
2. Search for and select the Active Locale ID.
3. Select the Time Zone ID from the drop-down menu.
4. Leave the **Always display Scheduled Offerings in this Time Zone** checkbox unchecked.
5. Click **Apply Changes**.



CONCLUSION

In this lesson, you were introduced to the admin management functionality and the key things to consider when creating a new admin account. Using the provided step-by-step instructions, you created a new admin.

You should now be able to:

- Identify the effect of a role on an admin account
- Apply multiple roles to an admin account

In the next lesson, you will take a deeper look at learner access in SATERN. .



LESSON CHECK

Use what you learned in this lesson to answer the following questions.

1. What is the limit to the number of roles that can be assigned to an admin?

2. If an admin account is not assigned a role, the admin will:
 - a) Not be able to log in.
 - b) Will have the ability to perform all functions.
 - c) Will be able to log in but have access to nothing.



Lesson 4:

Learner Access

The goal for this lesson is to provide information about learner access in the SATERN system.

OBJECTIVES

Upon completion of this lesson, you will be able to:

- Define the SATERN learner roles
- Define a catalog
- Identify how learners get access to catalogs

LEARNER ACCESS TO MENUS

Learner access to SATERN system menus is controlled with learner roles. A learner role contains workflows in much the same way as admin roles; however, there are no domain restrictions applied.

By selecting one or more learner workflows to add to a learner role, an admin may grant access to specific menu items and even entire menus.

SATERN Learner Roles

SATERN learner roles include:

- ◆ CONTRACTOR – assigned to contractor learners
- ◆ DEFAULT – assigned to civil service learners

LEARNER ACCESS TO ITEMS AND SCHEDULED OFFERINGS

Learner access to items and scheduled offerings is managed with catalogs.

Catalogs



Catalogs help control which items and which of their associated scheduled offerings are available to what learners. Catalogs are created under the Commerce menu. Access to a catalog is determined by assignment profiles.



Note: Creating and managing assignment profiles are discussed in the Learning Needs Management course.

An item can be added to one or more catalogs. New scheduled offering(s) of that item are added to those same catalogs by default. A scheduled offering of an item may be removed from any or all of the catalogs containing that item. However, a scheduled offering cannot be added to a catalog that does not already contain the item.

NASA Business Rule

Catalog IDs start with the center acronym followed by a hyphen, followed by all upper-case alpha or numeric characters.

Catalog ID:	ARC_CATALOG
Description:	Ames Research Center
<div> <div>Summary</div> <div>Items</div> <div>Curricula</div> <div>Assignment Profiles</div> </div>	
Edit the Catalog	
* = Required Fields	
Description:	<input type="text" value="Ames Research Center"/>
* Domain:	<input type="text" value="ARC"/>
Pricing Rule:	<input type="text" value=""/>
Active:	<input checked="" type="checkbox"/>
Contact Email:	<input type="text" value=""/>
<div> <div>Apply Changes</div> <div>Reset</div> <div>Delete</div> </div>	

Figure 8. Summary Tab of Catalog Record



Lab 2. Add a New Catalog

Step

1. Navigate to **Commerce > Catalogs**.
2. Click the **Add New** link.
3. Enter a catalog ID.
4. Enter a catalog description (**SATERN mandatory field**).
5. Select the **Items** tab.
6. Click **add one or more from list**.
7. Search for and select items to be placed in the catalog.
8. Select the **Curricula** tab.
9. Click **add one or more from list**.
10. Search for and select curricula to be place in the catalog.

GRANTING LEARNERS ACCESS TO A CATALOG

After the catalog is created and the desired items and curricula have been placed in it, we must still decide which learners have access to the catalog. To give learner(s) access to a catalog, you must create a new assignment profile or apply it to an existing assignment profile.



Note: Creating and managing assignment profiles are covered in the Learning Needs Management course.

NASA Business Rule

Only administrators with the “All” role or “Regional Admin Level 1” role have the authorized workflow to create an assignment profile. Therefore, any catalog creations for the disciplines, (e.g., ITS, SMA) must be created by an admin at the NASA Shared Services Center (NSSC), who has the authorized workflow. Assignment profiles for Center catalogs will be created by an admin at the Center who has the authorized workflow. The assignment profile shall follow the naming convention listed in the “Data Entry and Data Consistency” section of the *Business Rules Guide*).

If a learner is not included as part of any assignment profile, then no catalogs are displayed on the Catalog Preview tab of the learner record. Also, the learner would not be able to find any items and/or curricula when they would conduct a search on the learner side.



CONCLUSION

In this lesson, you were introduced to learner roles and catalogs. Using the step-by-step instructions, you created catalogs and granted learners access to the catalog.

You should now be able to:

- Define the SATERN learner roles
- Define a catalog
- Identify how learners get access to catalogs



LESSON CHECK

Use what you learned in this lesson to answer the following questions.

1. True or false:

An assignment profile must be created in order to give learners access to catalogs.

2. True or false:

SATERN has two different learner roles: Contractor and Default.



Course Summary

Through lecture, activities, and hands-on computer lab work, this course taught you the concepts and terminology associated with managing access in the SATERN system. You gained basic, hands-on experience using the system functions in order to create and modify the security structure.

You should now be able to:

- Describe the security model in SATERN
- Understand the purpose of domains and domain restrictions
- Describe learner roles and access to catalogs



Notes